7. GRÖBNER BASES

Theorem 7.1 (Hilbert's Basis Theorem)

Let $I \subset K[x_1, \ldots, x_n]$ be an ideal.

Then $\exists\, p_1, \ldots, p_s \in I$ such that $I = \langle p_1, \ldots, p_s \rangle$

Proof

$\{0\} = \langle 0 \rangle$, so we may assume $I \neq \{0\}$.

Fix an arbitrary monomial order $>$ and consider $\langle LT(I) \rangle$

Lemma 6.12 $\Rightarrow \langle LT(I) \rangle = \langle LT(p_1), \ldots, LT(p_s) \rangle$

for some $p_1, \ldots, p_s \in I$. Claim: $I = \langle p_1, \ldots, p_s \rangle$.

Proof of claim:

Let $f \in I$. By multivariate polynomial division

$$f = q_1 p_1 + \cdots + q_s p_s + r$$

and no term of r is divisible by $LT(p_1), \ldots, LT(p_s)$.

On the other hand

$$r = f - q_1 p_1 - \cdots - q_s p_s \in I,$$

so if $r \neq 0$ then $LT(r) \in LT(I) \subset \langle LT(p_1), \ldots, LT(p_s) \rangle$

which would contradict indivisibility of terms of r.

Hence $r = 0$ and $f \in \langle p_1, \ldots, p_s \rangle$. $\square$

Definition 7.2

Let $I \subset k[x_1, \dots, x_n]$ ideal and $>$ a monomial order.
A Gröbner basis of I is a finite subset $G = \{g_1, \dots, g_s\}$ such that

$$\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$$

Hilbert's Basis Theorem proof $\Rightarrow$ every ideal has a Gröbner basis for any monomial order.

(Convention: The zero ideal is generated by the empty set $\{0\} = \langle \emptyset \rangle$)

Lemma 7.3

$\{g_1, \dots, g_s\} \subset I$ is a Gröbner basis of I if and only if

$$p \in I \Rightarrow LT(g_i) \mid LT(p) \text{ for some } i = 1, \dots, s$$

Proof

"$\Rightarrow$" $p \in I \Rightarrow LT(p) \in LT(I) \subset \langle LT(g_1), \dots, LT(g_s) \rangle$

"$\Leftarrow$" Let $f \in \langle LT(I) \rangle$. Then $f = \sum_j h_j \, LT(p_j)$ for some $h_j \in k[x_1, \dots, x_n]$ and $p_j \in I$.

By assumption $LT(p_j) = LT(g_{i_j}) \cdot q_j$, $q_j \in k[x_1, \dots, x_n]$

$\Rightarrow f = \sum_j h_j q_j \, LT(g_{i_j}) \in \langle LT(g_1), \dots, LT(g_s) \rangle$ $\square$

Example 7.4

(1) Example 6.13 $\Rightarrow$ $p_1 = -t + x - 1$, $p_2 = -t^2 + y + 1$

is not a Gröbner basis of $\langle p_1, p_2 \rangle$ in lex order on $\mathbb{Q}[t,x,y]$

(2) Let $g_1 = x + z$, $g_2 = y - z$, $I = \langle g_1, g_2 \rangle$

Claim: g_1, g_2 is a Gröbner basis in lex order on $\mathbb{R}[x,y,z]$

Proof: Let $f \in I$, $f \neq 0$. We need to check that

$LT(f) \in \langle LT(g_1), LT(g_2) \rangle = \langle x, y \rangle$

If not, then $f = a_n z^n + a_{n-1} z^{n-1} + \dots + a_0$.

On the other hand, f vanishes on

$$V(g_1, g_2) = \{(-t, t, t) : t \in \mathbb{R}\} \subset \mathbb{R}^3$$

$\Rightarrow a_n t^n + a_{n-1} t^{n-1} + \dots + a_0 = 0 \quad \forall t \in \mathbb{R}$

$\Rightarrow a_n = \dots = a_0 = 0 \quad \Rightarrow \quad f = 0$,

which is a contradiction. Hence $LT(f) \in \langle LT(p_1), LT(p_2) \rangle$

Theorem 7.5 (The Ascending Chain Condition; ACC)

Let $I_0 \subset I_1 \subset I_2 \subset I_3 \subset \dots$ be ideals in $k[x_1, \dots, x_n]$

Then there exists $N \in \mathbb{N}$ such that $I_N = I_{N+1} = I_{N+2} = \dots$.

Proof

Consider $I_\infty := \bigcup_{n \in \mathbb{N}} I_n$.

The set I_∞ is an ideal:

- $0 \in I_0 \subset I_\infty$
- If $p, q \in I_\infty$ then $p \in I_n$ and $q \in I_m$, $n, m \in \mathbb{N}$
  Then $p, q \in I_{max(n,m)} \Rightarrow p+q \in I_{max(n,m)} \subset I_\infty$.
- If $p \in I_\infty$ and $q \in k[x_1, \dots, x_n]$, then $p \in I_n$, $n \in \mathbb{N}$
  $\Rightarrow pq \in I_n \subset I_\infty$

Hilbert's Basis Theorem $\Rightarrow I_\infty = \langle p_1, \dots, p_s \rangle$ for some $p_1, \dots, p_s \in I_\infty$.

For each $i = 1, \dots, s$ there is some $n_i \in \mathbb{N}$, $p_i \in I_{n_i}$

Let $N = \max\{n_i : i = 1, \dots, s\}$. Then

$$I_\infty = \langle p_1, \dots, p_s \rangle \subset I_N \subset I_\infty \Rightarrow I_N = I_{N+1} = \dots = I_\infty \quad \square$$

Note: ACC $\Rightarrow$ Hilbert's Basis Theorem

since an ideal without a finite basis would give

a sequence $\langle p_1 \rangle \subsetneq \langle p_1, p_2 \rangle \subsetneq \langle p_1, p_2, p_3 \rangle \subsetneq \dots$

Definition 7.6

Let $I \subset k[x_1, \dots, x_n]$ be an ideal.

The variety of the ideal I is

$$V(I) = \{(a_1, \dots, a_n) \in k^n : p(a_1, \dots, a_n) = 0 \ \forall p \in I\}$$

Proposition 7.7

$V(I)$ is a variety, i.e. $V(I) = V(g_1, \dots, g_s)$ for some $g_1, \dots, g_s \in k[x_1, \dots, x_n]$.

Proof

Hilbert's Basis Theorem $\Rightarrow$ $I = \langle g_1, \dots, g_s \rangle$.

Then $V(I) \subset V(g_1, \dots, g_s)$ since $g_1, \dots, g_s \in I$.

For the converse, let $a \in V(g_1, \dots, g_s) \subset k^n$

Then for any $f \in I$, write $f = \sum h_i g_i$

$$\Rightarrow f(a) = \sum h_i(a) g_i(a) = \sum h_i(a) \cdot 0 = 0$$

$$\Rightarrow a \in V(I) \quad \square$$

Proposition 7.8

Let $I \subset k[x_1, \ldots, x_n]$ an ideal and $G = \{g_1, \ldots, g_s\} \subset I$ a Gröbner basis. Then $\forall f \in k[x_1, \ldots, x_n]$ $\exists! r \in k[x_1, \ldots, x_n]$ such that $f - r \in I$ and no term of r is divisible by $LT(g_1), \ldots, LT(g_s)$.

Proof

Existence of r follows from the division algorithm:

$$f = q_1 g_1 + \cdots + q_s g_s + r$$

For uniqueness, suppose

$$f = g + r = \tilde{g} + \tilde{r}$$

with $g, \tilde{g} \in I$ and all terms of $r, \tilde{r}$ not divisible by $LT(g_i)$

If $r \neq \tilde{r}$, then $0 \neq r - \tilde{r} \in I$

$\Rightarrow LT(r - \tilde{r}) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle$

Lemma 6.2 $\Rightarrow$ $LT(g_i) \mid LT(r - \tilde{r})$ for some i.

The monomial $LM(r - \tilde{r})$ must appear in either r or $\tilde{r}$, so $LT(g_i)$ divides a term of r or $\tilde{r}$.

Hence $r = \tilde{r}$ and we have uniqueness. $\square$

Corollary 7.9

Let $G = \{g_1, \dots, g_s\}$ be a Gröbner basis of I. Then $f \in I \iff$ the remainder of division of f by G is zero.

Proof

By Proposition 7.8 the decomposition

$$f = g + r, \quad g \in I, \quad r \text{ remainder}$$

is unique.

"$\Leftarrow$" If $r = 0$, then $f = g \in I$.

"$\Rightarrow$" If $f \in I$, then $g + r = f + 0$ is a valid decomposition, so by uniqueness $r = 0$.

Definition 7.10

Let $f \in K[x_1, \dots, x_n]$, $P = (p_1, \dots, p_s)$, $p_i \in K[x_1, \dots, x_n]$. Let $r \in K[x_1, \dots, x_n]$ be the remainder of the division algorithm for f by the tuple P.

We denote

$$\overline{f}^P = r$$

If $G = (p_1, \dots, p_s)$ is a Gröbner basis of $\langle G \rangle$ we will also denote

$$f \rightarrow_G r$$

"f reduces to r mod G"

Definition 7.11

Let $p, q \in K[x_1, \ldots, x_n]$ and $>$ a monomial order.

Let $\alpha = (\alpha_1, \ldots, \alpha_n) = \text{multideg } p$ and $\beta = (\beta_1, \ldots, \beta_n) = \text{multideg } q$

(i) The least common multiple of $LM(p) = x^\alpha$ and $LM(q) = x^\beta$ is

$$\text{lcm}(LM(p), LM(q)) = x^\gamma,$$

where $\gamma = (\gamma_1, \ldots, \gamma_n)$, $\gamma_i = \max(\alpha_i, \beta_i)$

(ii) The S-polynomial of p and q is

$$S(p,q) = \frac{x^\gamma}{LT(p)} \cdot p - \frac{x^\gamma}{LT(q)} \cdot q$$

Example 7.12

Let $p_1 = -t + x - 1$, $p_2 = -t^2 + y + 1$ in lex order on $\mathbb{Q}[t, x, y]$ from Example 5.11.

Then $LM(p_1) = t$ $LM(p_2) = t^2$, so

$$x^\gamma = \text{lcm}(t, t^2) = t^2.$$

Then

$$S(p_1, p_2) = \frac{t^2}{-t}(-t + x - 1) - \frac{t^2}{-t^2}(-t^2 + y + 1)$$

$$= -tx + t + y + 1$$

Let $f = x^2 - 2x - y$, $LM(f) = x^2$, $\text{lcm}(t, x^2) = tx^2$

Then

$$S(p_1, f) = \frac{tx^2}{-t}(-t + x - 1) - \frac{tx^2}{x^2}(x^2 - 2x - y)$$

$$= 2tx + ty - x^3 + x^2$$

Lemma 7.13

Let $p_1, \dots, p_s \in K[x_1, \dots, x_n]$, $\text{multideg}(p_1) = \dots = \text{multideg}(p_s) = \delta$

(i) multideg $S(p_i, p_j) < \delta$ for all i, j

(ii) If $\text{multideg}\left(\sum_{i=1}^{s} p_i\right) < \delta$, then $\sum_{i=1}^{s} p_i$ is a K-linear combination of the $S(p_i, p_j)$, i, j.

Proof

Let $d_i := LC(p_i)$, so $LT(p_i) = d_i x^\delta$.

(i) $\text{lcm}(LM(p_i), LM(p_j)) = \text{lcm}(x^\delta, x^\delta) = x^\delta$, so

$$S(p_i, p_j) = \frac{1}{d_i} p_i - \frac{1}{d_j} p_j = (x^\delta + \dots) - (x^\delta + \dots)$$

$\Rightarrow$ multideg $S(p_i, p_j) < \delta$.

(ii) The coefficient of x^δ in $\sum_{i=1}^{s} p_i$ is

$$d_1 + \dots + d_s = 0 \implies d_1 + \dots + d_{s-1} = -d_s$$

Hence

$$\sum_{i=1}^{s-1} d_i S(p_i, p_s) = d_1\left(\frac{1}{d_1} p_1 - \frac{1}{d_s} p_s\right) + \dots + d_{s-1}\left(\frac{1}{d_{s-1}} p_{s-1} - \frac{1}{d_s} p_s\right)$$

$$= p_1 + \dots + p_{s-1} - \frac{1}{d_s}(d_1 + \dots + d_{s-1}) p_s$$

$$= p_1 + \dots + p_s \quad \square$$

Theorem 7.14 (Buchberger's criterion)

Let $I \subset k[x_1, \dots, x_n]$ be an ideal and $G = \{g_1, \dots, g_t\}$ a basis of I.
Then G is a Gröbner basis of I if and only if the remainder $\overline{S(g_i, g_j)}^G$ is zero for all i, j.

Proof

"$\Rightarrow$" Since $S(g_i, g_j) \in I$, Corollary 7.9 $\Rightarrow$ $\overline{S(g_i, g_j)}^G = 0$